Criminal Liability for AI-Based Deepfake Pornography Offenders in Indonesia and South Korea

Ajeng Putri Berliana[1], Sinarianda Kurnia H.[2]
[1]ajengputribr@gmail.com ,[2]sinar@ubhara.ac.id
Universitas Bhayangkara Surabaya

ABSTRACT

The rapid advancement of Artificial Intelligence (AI) brings both benefits and challenges. While AI offers significant ease in various aspects of human life, it also contributes to the emergence of new crimes, such as identity forgery for illegal gain through Deepfake technology. The increasing sophistication of Deepfakes has raised serious concerns, especially with their misuse in the form of Deepfake Pornography. This phenomenon poses a growing threat to social media users and has drawn widespread public and governmental attention. This research employs a normative legal approach, focusing on statutory regulations and relevant legal doctrines. The study compares legal responses to Deepfake Pornography in Indonesia *and South Korea. In* Indonesia*, there is no specific law addressing Deepfake Pornography; thus, existing laws such as Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 44 of 2008 on Pornography, and Law No. 12 of 2022 are applied. Conversely, South Korea addresses this issue through the Criminal Law Act No. 20908 of 2025 and the Sexual Violence Punishment Act No. 20459. The study finds that both countries have made efforts to respond to the threat of Deepfake Pornography, yet each legal system has its own strengths and weaknesses. This comparative analysis aims to provide insight into the effectiveness of current legal frameworks and to contribute to the development of more comprehensive and responsive regulations.*

Keywords: *Artificial Intelligence, Criminal liability, Deepfake Porn*

Pertanggungjawaban Pidana Pelaku *Deepfake Porn* Berbasis *Artificial Intelligence* di Indonesia dan Korea Selatan

ABSTRAK

Perkembangan Artificial Intelligence (AI) membawa dampak positif sekaligus tantangan baru. Di satu sisi, AI mempermudah kehidupan manusia, namun di sisi lain menimbulkan kejahatan baru seperti pemalsuan identitas demi keuntungan ilegal melalui teknologi Deepfake. Semakin canggihnya teknologi Deepfake menimbulkan kekhawatiran serius, terutama penyalahgunaannya dalam bentuk pornografi. Fenomena ini menjadi ancaman yang berkembang bagi pengguna media sosial dan menarik perhatian publik serta pemerintah. Penelitian ini menggunakan pendekatan yuridis normatif dengan fokus pada peraturan perundang-undangan serta doktrin hukum yang relevan. Penelitian ini membandingkan penanganan hukum terhadap Deepfake Porn di Indonesia *dan* Korea Selatan. *Di* Indonesia, *belum terdapat pengaturan khusus mengenai Deepfake Porn, sehingga penanganannya mengacu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, dan Undang-Undang Nomor 12 Tahun 2022. Sementara itu,* Korea Selatan *mengatur permasalahan ini melalui Criminal Law Act No. 20908 Tahun 2025 dan Sexual Violence Punishment Act No. 20459. Penelitian ini menemukan bahwa kedua negara telah berupaya menanggapi ancaman Deepfake Porn, namun masing-masing sistem hukum memiliki kelebihan dan kekurangannya. Analisis ini bertujuan memberikan gambaran efektivitas kerangka hukum yang ada dan mendorong pembentukan regulasi yang lebih komprehensif dan responsif.*

Kata kunci: *Artificial Intelligence, Deepfake Porn, Pertanggungjawaban Pidana*

INTRODUCTION

Technological advancement constitutes an inseparable dimension of human civilization. In contemporary life, technology has assumed a central role in sustaining a wide range of human activities and necessities, a condition that has emerged in parallel with the growth of scientific knowledge. This progression has brought humanity into the era of Industry 5.0, a paradigm centered on human values and driven by emerging technologies, among which Artificial Intelligence (AI) occupies a particularly prominent position.[1]

Artificial Intelligence refers to a class of systems engineered to replicate the cognitive capacities of living beings in order to address complex problems. This technology develops computer systems and machine devices to a degree of intelligence comparable to human reasoning and operation.[2] The rapid development of Artificial Intelligence carries considerable consequences, both beneficial and detrimental. While AI has the capacity to simplify and enhance human life, it simultaneously opens new avenues for criminal exploitation, including identity fraud aimed at unlawful gain, a phenomenon exemplified by Deepfake technology.[3]

Deepfake is a product of deep learning technology employed to generate synthetic or counterfeit content.[4] It functions as a media synthesis technology that harnesses Artificial Intelligence to fabricate visual representations of individuals by processing and manipulating image or video data, thereby producing digital constructs that appear authentic and are difficult to distinguish from genuine material. As this technology continues to mature, the capacity of Artificial Intelligence to generate increasingly convincing fabricated content will correspondingly intensify.[5]

Deepfake technology does not yield exclusively positive outcomes; rather, it introduces a distinct set of challenges that warrant serious attention. On one hand, its sophistication can be directed toward entertainment, including the production of

---

[1] Wahyudi BR, "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI," *Innovative: Journal Of Social Science Research* 5, no. 1 (January 25, 2025): 3436–50, https://doi.org/10.31004/INNOVATIVE.V5I1.17519.

[2] Muhammad Rizki Kurniarullah et al., "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi," *Jurnal Ilmiah Wahana Pendidikan* 10, no. 10 (June 3, 2024): 534–47, https://doi.org/10.5281/ZENODO.11448814.

[33] Chiquita Thefirstly Noerman and Aji Lukman Ibrahim, "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara," *JURNAL USM LAW REVIEW* 7, no. 2 (June 3, 2024): 603–21, https://doi.org/10.26623/JULR.V7I2.8995.

[4] Sabrina Nur Syahirah and Bayu Prasetyo, "TINJAUAN YURIDIS TERHADAP PENGGUNAAN TEKNOLOGI DEEPFAKE UNTUK PORNOGRAFI MELALUI ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA," *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (February 13, 2025): 191–212, https://ejurnals.com/ojs/index.php/jihk/article/view/1405.

[5] Hendra Prayoga and Hadi Tuasikal, "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia," *Abdurrauf Law and Sharia* 2, no. 1 (May 1, 2025): 22–38, https://doi.org/10.70742/ARLASH.V2I1.194.

creative and engaging video content. On the other hand, Deepfake poses tangible threats to individual reputation, serves as a vehicle for fraud, and may even facilitate extortion.[6] Irresponsible actors have exploited Deepfake technology to manipulate images or videos by superimposing the faces of other individuals onto existing footage. Such content has frequently been deployed to damage the reputations of public figures and to shape public opinion in misleading directions, thereby posing a significant threat to social stability.[7]

At present, Deepfake pornography has emerged as a serious concern with far-reaching consequences across both the pornography industry and society at large. Victims endure a range of severe harms, including psychological distress, reputational damage within their communities, and violations of their personal privacy and security.[8] Women constitute the overwhelming majority of Deepfake pornography victims. According to the 2023 Deepfake Production Status report published by cybersecurity firm Security Hero, 99 percent of Deepfake pornographic videos target women.[9] Furthermore, data from the same organization reveals a dramatic rise in AI-generated adult content, from 3,725 cases in 2022 to 21,019 cases in 2023, reflecting an increase of 464 percent within a single year.[10]

Indonesia, in particular, has yet to establish a legal instrument that explicitly regulates and imposes sanctions upon the practice of Deepfake pornography.[11] This absence of specific regulation creates a legal vacuum (*rechtsvacuum*) that obstructs law enforcement authorities in prosecuting perpetrators with precision and in providing adequate remedies for victims. By contrast, South Korea has enacted explicit criminalization of Deepfake pornography through Article 14-2 of the Act on Special Cases Concerning the Punishment of Sexual Crimes, which encompasses acts of creating, altering, distributing, possessing, and purchasing Deepfake pornographic content. This legislative development is particularly significant given that South Korea

---

[6] Rendi Syaputra Nur Haida and Eko Nuriyatman, "URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI ARTFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA," *Jurnal Hukum Respublica* 24, no. 01 (December 5, 2024): 1–13, https://doi.org/10.31849/RESPUBLICA.V24I01.23327.

[7] Yoan Shevila Kristiyenda, Jasmine Faradila, and Christina Basanova, "Pencegahan Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (March 4, 2025): 149–64, https://doi.org/10.59246/ALADALAH.V3I2.1263.

[8] Mahrus Ali et al., "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims," *Substantive Justice International Journal of Law* 8, no. 1 (May 15, 2025): 1–12, https://doi.org/10.56087/SUBSTANTIVEJUSTICE.V8I1.306.

[9] "2023 State Of Deepfakes: Realities, Threats, And Impact," 2023, https://www.securityhero.io/state-of-deepfakes/#deepfake-porn-survey.

[10] "2023 State Of Deepfakes: Realities, Threats, And Impact."

[11] Muhammad Faturrachman SY, "DEEPFAKE PORNOGRAFI: STUDI KONSTITUSI DAN PENEGAKANNYA DI INDONESIA," *Jurnal Legislatif* 8, no. 2 (January 14, 2025): 113–28, https://doi.org/10.30659/JHKU.V19I4.43173.

ranks as the country with the highest concentration of Deepfake pornographic content globally, with 53 percent of victims appearing in such material worldwide being South Korean nationals.[12] In a 2024 gender-violence study finds that in 2023, a Deepfake report shows that from 100.000 of face-swap porn videos, 53% victims are Soiuth Korean woman.[13]

Prior scholarly inquiry into technology-based cybercrime within the framework of criminal law has been conducted by several researchers. Suartika et al. examined legal policy concerning acts of exhibitionism conducted through video call-based social media platforms, analyzed through the lens of the Electronic Information and Transactions Law (Undang-Undang Informasi dan Transaksi Elektronik). That study offered an account of how Indonesian positive law responds to sexual offenses that exploit digital platforms.[14] Separately, Hartono and Sugiharto investigated criminal liability for perpetrators who produce and disseminate pornographic videos through social media, employing a digital forensics approach as a framework for evidentiary analysis.[15]

The present study is distinguished from these prior works by virtue of its specific subject matter. Earlier research has concentrated on conventional social media-based pornographic offenses and their evidentiary dimensions, whereas this study focuses specifically on criminal liability for perpetrators of AI-based Deepfake pornography through a comparative legal analysis of Indonesia and South Korea, including an examination of the respective strengths and limitations of the legal frameworks in both jurisdictions.

In light of the issues elaborated above, this study seeks to examine the criminal liability of perpetrators of AI-based Deepfake pornography in Indonesia and South Korea, as well as the strengths and weaknesses of the legal arrangements governing Deepfake pornographic offenses in both countries.

RESEARCH METHODOLOGY

[12] Xiangshu Cheng, "The Gendered Impact of Deepfake Technology: Analyzing Digital Violence Against Women in South Korea," *Lecture Notes in Education Psychology and Public Media* 75, no. 1 (November 26, 2024): 80–85, https://doi.org/10.54254/2753-7048/75/20241102.

[13] Cheng, "The Gendered Impact of Deepfake Technology: Analyzing Digital Violence Against Women in South Korea."

[14] I Komang Suarsika, Ni Ketut Wiratny, and Erikson Sihotang, "LEGAL POLICY ON EXHIBITIONISM THROUGH VIDEO CALL-BASED SOCIAL MEDIA REVIEWED FROM THE INFORMATION AND ELECTRONIC TRANSACTIONS (IET) LAW," *IUS POSITUM: Journal of Law Theory and Law Enforcement* 3, no. 2 (August 9, 2024): 48–61, https://doi.org/10.56943/JLTE.V3I2.576.

[15] Dhimas Joeantito Hartono and Sugiharto Sugiharto, "THE CRIMINAL RESPONSIBILITY FOR PORNOGRAPHY VIDEO MAKER THROUGH DIGITAL FORENSICS ON SOCIAL MEDIA," *YURIS: Journal of Court and Justice* 1, no. 2 (August 1, 2022): 46–54, https://doi.org/10.56943/JCJ.V1I2.119.

This study adopts a normative legal research approach (doctrinal legal research) as its primary method for analyzing the legal issues under examination. The study analyzes various written legal materials as forms of positive law, with particular emphasis on those pertaining to the criminal offense of Deepfake pornography. The research centers on a systematic analysis of written legal sources relevant to Deepfake pornographic offenses, with the aim of elucidating the juridical foundations and legal provisions that bear upon the issues addressed in this study.

RESULTS AND DISCUSSION

Criminal Liability of Deepfake Pornography Perpetrators in Indonesia and South Korea

Within any legal system, criminal liability functions as a juridical instrument for assessing the legal capacity (*rechtsvermogen*) of an individual to bear the legal consequences arising from a criminal act. In its most fundamental sense, this concept serves as the basis for determining whether a person suspected of committing a criminal offense is to be acquitted or subjected to criminal punishment in accordance with applicable law. Criminal liability, however, is not merely a technical legal construct. It cannot be separated from the architecture of moral values and ethical norms that are embedded in society, given that criminal law serves as a mechanism of social control. This orientation ensures that justice is genuinely upheld throughout every stage of the legal process. Within the criminal law system, criminal liability represents the principle that places the burden of accountability for a criminal act upon the perpetrator who has violated the rule of law. An individual is considered criminally liable when his or her conduct satisfies the element of unlawfulness. Both Indonesian and South Korean courts adhere to subjective and objective elements as recognized under their respective criminal codes. The objective element pertains to those factors inherent in the perpetrator, while the subjective element concerns the acts committed and the consequences borne by the perpetrator.[16] Nonetheless, the terminology and emphasis applied to each of these elements may differ between the two jurisdictions.[17]

Indonesia does not yet possess specific legal provisions governing Deepfake technology. In principle, the misuse of Deepfake falls within the broader category of cybercrime; accordingly, the applicable regulatory framework encompasses legislation concerning electronic information, pornography, and sexual violence offenses. The

[16] Anselmus S. J. Mandagie, "PROSES HUKUM TINDAK PIDANA PEMBUNUHAN YANG DILAKUKAN OLEH ANAK DIBAWAH UMUR DITINJAU DARI UNDANG-UNDANG NOMOR 11 TAHUN 2012 TENTANG SISTEM PERADILAN PIDANA ANAK," *LEX CRIMEN* 9, no. 2 (May 18, 2020), https://ejournal.unsrat.ac.id/v2/index.php/lexcrimen/article/view/28552.
[17] Jung Seong Geun and Jung Jun Seob, *Pengantar Pelajaran Hukum Pidana* (Seoul: Parkyoungsa, 2019).

legal instruments most commonly invoked in addressing Deepfake pornography cases in Indonesia include Law Number 1 of 2024, Law Number 19 of 2016, and Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). In this context, Deepfake pornography aligns with the definition set out in Article 1 Number 8 of Law Number 19 of 2016, which provides that an electronic agent constitutes a component of an electronic system designed to perform specific actions on electronic information, operated either by a human or by a designated party.[18][19]

The operator of an electronic agent bears full legal responsibility for all legal consequences arising from the operation of the electronic system under its management, in accordance with applicable statutory provisions. Artificial Intelligence cannot yet be classified as a legal subject (legal subject) due to its inability to satisfy the fundamental elements of legal accountability. This is attributable to the incapacity of Artificial Intelligence to comprehend knowledge or to form subjective intent. Legal scrutiny must therefore be directed at the human actors who have deployed Artificial Intelligence for harmful and malicious purposes to the detriment of others. Deepfake pornography satisfies the constituent elements of Article 27 Paragraph (1) of Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, which may be interpreted as follows: the perpetrator constitutes a subject who may be held criminally liable; the conduct in question involves the distribution and production of publicly accessible content; the material contravenes public decency by featuring sexual exploitation; and the content is disseminated through digital platforms in a manner that renders it publicly accessible without the victim's consent.[20]

With respect to the sanctions applicable to Deepfake pornography perpetrators, Article 45 Paragraph (1) of Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions stipulates that perpetrator may be sentenced to a maximum of six years of imprisonment and/or a fine of up to Rp1,000,000,000 (one billion rupiah).[21]

This provision is further reinforced by Article 14 Paragraph (1) of Law Number 12 of 2022 on the Crime of Sexual Violence, which provides that any person who records and/or captures images or screenshots of a sexual nature without the consent

[18] Pemerintah Pusat Indonesia, "Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Pemerintah Pusat* (Jakarta, November 25, 2016), https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016.
[19] Pemerintah Pusat Indonesia, "Undang-Undang (UU) Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2008, https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008.
[20] Pemerintah Pusat Indonesia, "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik" (Jakarta, 2024), https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024.
[21] Indonesia, "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."

or against the will of the subject of such recording or image; transmits electronic information and/or electronic documents of a sexual nature against the will of the recipient and directed at satisfying sexual desire; and/or conducts surveillance and/or tracking through electronic systems of the subject of an electronic information or document for sexual purposes, shall be convicted of electronic-based sexual violence, punishable by a maximum of four years of imprisonment and/or a fine of up to Rp200,000,000 (two hundred million rupiah). [22]

Deepfake pornography perpetrators may be subject to these criminal sanctions on the grounds that their conduct satisfies the element of capturing images or screenshots of a sexual nature without the consent of the person depicted. However, the provision's definition of electronic-based sexual offenses refers exclusively to acts of recording and/or image capture, as well as the distribution of photographs and videos obtained without the victim's consent, and therefore does not specifically address the use of Artificial Intelligence technologies such as Deepfake.

In South Korea, Deepfake-related offenses are not confined to any particular demographic. Individuals of any gender, age, or occupation may become victims. Deepfake pornography may be prosecuted under Article 283 of Law Number 20908 of 2025 on the Criminal Act, which provides that any person who threatens another shall be subject to imprisonment for a period not exceeding three years, a fine not exceeding five million won, detention, or a minor fine.[23]

Deepfake pornography is also subject to Article 14-2 of Law Number 20459 on the Punishment of Sexual Violence Crimes, which stipulates as follows:

1. Any person who edits, synthesizes, or processes film, video, or audio material featuring the face, body, or voice of another person into a form that may provoke sexual arousal or shame, against the will of the subject of such material, shall be punishable by imprisonment for a period not exceeding seven years or a fine not exceeding fifty million won.
2. Any person who distributes a compilation, composite, or processed work (an edited work) or reproduction thereof under paragraph (1), or who distributes such work or its reproduction after the fact against the will of the subject of the video material, even where the editing under paragraph (1) was not conducted against the will of that subject, shall be punishable by imprisonment for a period not exceeding seven years or a fine not exceeding fifty million won.
3. Any person who commits the offense under paragraph (2) through the use of an information and communications network for the purpose of gain, against the

[22] Pemerintah Pusat Indonesia, "Undang-Undang (UU) Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual" (Jakarta, 2022), https://peraturan.bpk.go.id/Details/207944/uu-no-12-tahun-2022.
[23] "CRIMINAL ACT," Pub. L. No. 19582, Ministry of Government legislation (2023), https://www.law.go.kr/eng/engLsSc.do?menuId=2&query=#liBgcolor10.

will of the person receiving the video material, shall be punishable by a fixed-term imprisonment of not less than three years.

4. Any person who possesses, purchases, stores, or views a compilation or reproduction thereof under paragraph (1) or (2) shall be punishable by imprisonment for a period not exceeding three years or a fine not exceeding thirty million won.
5. Where the offenses enumerated in paragraphs (1) through (3) are committed on a habitual basis, the prescribed punishment shall be increased by up to one-half of the penalty stipulated for each respective offense.[24]

Strengths and Weaknesses of the Legal Regulation of Deepfake Pornography Offenses in Indonesia and South Korea

The resolution of Deepfake pornography offenses varies considerably across different national jurisdictions, as is evident in the contrasting approaches adopted by Indonesia and South Korea. As elaborated in the preceding discussion, both countries maintain their respective regulatory frameworks for addressing this category of offense, each of which carries distinct advantages and limitations.

1. Indonesia

   The absence of specific legislation governing AI-based Deepfake pornography in Indonesia has led law enforcement authorities to rely upon existing general provisions to prosecute Deepfake pornography perpetrators, including Article 27 Paragraph (1) of Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, Article 4 Paragraph (1) of Law Number 44 of 2008 on Pornography, and Article 14 Paragraph (1) of Law Number 12 of 2022 on the Crime of Sexual Violence.

   By not being bound to a narrow statutory definition, law enforcement authorities are not constrained exclusively to the definition of Deepfake pornography. This flexibility permits adaptation to the continuously evolving modalities of emerging criminal conduct as technology advances.[25] Without being tied to a single specific statute, law enforcement may select and apply the most contextually relevant provisions from a range of legislative instruments depending on the nature of each case. This approach simultaneously serves a preventive function against over-regulation of technology that remains in active

[24] "ACT ON SPECIAL CASES CONCERNING THE PUNISHMENT OF SEXUAL CRIMES," Pub. L. No. 20575, Ministry of Government legislation (2025), https://www.law.go.kr/eng/engLsSc.do?menuId=2&query=punishment#liBgcolor7.

[25] Sindi Ayu Andira and M. Endriyo Susila, "Overcoming Deepfake Porn Crimes In Indonesia," *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 23, no. 1 (June 28, 2024): 2796–2809, https://doi.org/10.31941/PJ.V23I3.4232.

development. Overly restrictive regulation risks impeding innovation in the fields of Artificial Intelligence and multimedia, and may introduce excessive censorship of creative content that constitutes a legitimate exercise of freedom of expression, including parody, satire, and digital artistic works.[26]

On the other hand, Indonesia continues to face several fundamental weaknesses in the regulation of this category of offense. To date, Indonesia lacks a specific and comprehensive regulatory framework governing the misuse of Deepfake technology, resulting in a continued dependence on general provisions that are insufficiently equipped to address the full complexity of AI-based Deepfake pornography offenses.[27] This regulatory deficiency has a direct impact on the inadequacy of victim protection measures currently in place.

The implementation of existing regulations remains constrained by limited comprehension among law enforcement personnel, the absence of effective victim recovery mechanisms, and the lack of a dedicated institutional body for the rehabilitation of victims of electronic-based sexual violence. As a consequence, victims frequently encounter substantial difficulties in removing content that has already been widely disseminated across digital platforms, face procedural barriers in the prosecution of perpetrators due to the evidentiary challenges inherent in establishing the manipulation of digital content, and fail to receive adequate psychological rehabilitation or financial compensation.[28] Furthermore, the legal responsibility of digital platforms has not been clearly defined. The absence of statutory provisions mandating platforms to prevent and address the spread of Deepfake pornographic content means that platforms cannot be held legally accountable, notwithstanding the fact that in practice they serve as the primary medium through which such content is disseminated. Ideally, digital platforms should be under an obligation to remove violating content expeditiously, protect victim privacy, conduct public education initiatives, and provide responsive reporting mechanisms.[29]

---

[26] Jon Truby, "Governing Artificial Intelligence to Benefit the UN Sustainable Development Goals," *Sustainable Development* 28, no. 4 (July 1, 2020): 946–59, https://doi.org/10.1002/SD.2048;PAGE:STRING:ARTICLE/CHAPTER.

[27] Muhammad Faqih and Enni Soerjati Priowirjanto, "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia," *Jurnal Indonesia Sosial Teknologi* 3, no. 11 (November 24, 2022): 1156–68, https://doi.org/10.59141/JIST.V3I11.528.

[28] Angelica Vanessa Audrey Nasution, Suteki, and Anggita Doramia Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (October 1, 2025): 2489–2517, https://doi.org/10.1007/S11196-025-10265-0.

[29] Faqih and Priowirjanto, "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia."

2. South Korea

South Korea demonstrates several notable strengths in its regulation of Deepfake pornography offenses. The country has established a relatively comprehensive legal framework, featuring substantive regulations that specifically govern AI-based Deepfake pornography offenses, thereby providing a strong juridical basis for victim protection and the prosecution of perpetrators. In addition, South Korea has adopted a proactive approach to law enforcement.[30] Law Number 20459 on the Punishment of Sexual Violence Crimes encourages the use of active investigative methods, including online surveillance and undercover operations, to detect the spread of Deepfake pornographic content while observing the principles of human rights protection.[31] In practice, the competent authorities routinely monitor digital platforms, including Telegram, the dark web, and other closed forums, and have developed Deepfake content detection technologies in collaboration with the private sector.[32] The South Korean Ministry of Science and Information and Communication Technology, for instance, has pursued the development of dedicated algorithms for the automated scanning of illegal content, coupled with direct reporting to law enforcement agencies.

In the domain of victim protection, South Korea has also demonstrated concrete commitment. South Korean law affords more robust protection to victims, including those of AI-based Deepfake pornography offenses. Proactive measures such as online investigation and the protection of victim information have been proposed as means of preventing the harms associated with this category of offense.[33]

The South Korean government has furthermore implemented concrete steps to protect victims, including the launch of a seven-month law enforcement campaign directed at perpetrators who exploit children and adolescents.[34] Announced in August 2024 in response to the widespread proliferation of Deepfake content, this campaign actively conducted national operations to combat digital sexual crimes, with particular focus on the vulnerable

[30] Bu-gon Ryu, "Legal and Institutional Improvement Measures for the Protection of Victims of Deepfake Sex Crimes," 피해자학연구 32, no. 3 (December 31, 2024): 29–56, https://doi.org/10.36220/KJV.2024.32.3.29.
[31] Ryu, "Legal and Institutional Improvement Measures for the Protection of Victims of Deepfake Sex Crimes."
[32] Hyung-Jin Kim, "South Korea Fights Deepfake Porn with Tougher Punishment and Regulation," AP News, November 6, 2024, https://apnews.com/article/south-korea-deepfake-porn-women-409516f159827770913ddf8d39f84cfd.
[33] Yujin Jang and Youngmeen Suh, "Cyber Sex Crimes Targeting Children and Adolescents in South Korea: Incidents and Legal Challenges," *Social Sciences 2024, Vol. 13, Page 596* 13, no. 11 (November 3, 2024): 596, https://doi.org/10.3390/SOCSCI13110596.
[34] Jang and Suh, "Cyber Sex Crimes Targeting Children and Adolescents in South Korea: Incidents and Legal Challenges."

demographic of children and adolescents in the context of AI-based Deepfake pornographic content.[35] The campaign aimed to identify and apprehend perpetrators involved in the creation, distribution, or possession of Deepfake pornographic content without the victims' consent; to protect victims, particularly children and adolescents, from digital sexual crimes; and to raise public awareness regarding the dangers and consequences of Deepfake pornography.[36]

Notwithstanding these strengths, the legal framework in South Korea is also subject to certain weaknesses that merit careful consideration. First, the limited scope of existing legislation constitutes a principal concern. Article 14-2 of Law Number 20459 on the Punishment of Sexual Violence Crimes does not yet address forms of Deepfake technology misuse outside the context of video material, such as manipulated images produced for purposes of sexual harassment, thereby leaving gaps in legal enforcement and protection.[37] Second, the regulatory framework lags considerably behind the pace of technological development. Legislative processes typically require two to three years to complete, whereas Deepfake technology evolves at a rate that far exceeds the capacity of the legislative mechanism. The emergence of NeRF and Deep Voxel technologies for three-dimensional Deepfake in 2023, merely one year after the introduction of Stable Diffusion as a generative AI image platform, illustrates the extraordinary velocity of this technological progression. The increasing sophistication of Deepfake technology has facilitated the production and dissemination of Deepfake pornographic content by individuals with no specialized technical knowledge. While Deepfake technology does not invariably give rise to entirely novel legal problems, it tends to exacerbate pre-existing challenges and consistently demands regulatory responses that are more adaptive and responsive to the dynamics of technological change

This state of affairs indicates that both Indonesia and South Korea still face substantial challenges in aligning their legal systems with the continuously evolving dynamics of Deepfake technology. Accordingly, adaptive regulatory reform, the strengthening of victim protection mechanisms, and the clarification of digital platform responsibility constitute urgent priorities for both countries if they are to provide more effective legal certainty in combating AI-based Deepfake pornography offenses.

[35] Seung Gyeong Ji, "#MeToo in an AI-Generated Deepfake Sexual Violence Era in South Korea," *Women's Studies International Forum* 112 (September 1, 2025): 103146, https://doi.org/10.1016/J.WSIF.2025.103146.
[36] Ryu, "Legal and Institutional Improvement Measures for the Protection of Victims of Deepfake Sex Crimes."
[37] Kyungsuk Kim, "Deepfakes: Challenges to Intellectual Property Rights in South Korea," *GRUR International* 74, no. 6 (July 23, 2025): 532–42, https://doi.org/10.1093/GRURINT/IKAF044.

CONCLUSION

Several conclusions may be drawn from the preceding discussion. First, criminal liability for Deepfake pornography perpetrators requires the fulfillment of the constituent elements of the criminal offense as well as the perpetrator's capacity to be held accountable for his or her conduct. In Indonesia, criminal liability for Deepfake pornography perpetrators is grounded in the provisions of the ITE Law, the Pornography Law, and the Law on the Crime of Sexual Violence, whereas in South Korea it is governed by Law Number 20908 of 2025 on the Criminal Act and Law Number 20459 on the Punishment of Sexual Violence Crimes. Second, the regulation of Deepfake pornography in Indonesia carries the advantage of flexibility in legal interpretation and the prevention of over-regulation; however, it is undermined by the absence of specific legislation, inadequate victim protection, and the absence of clearly defined accountability for digital platforms. South Korea, by contrast, holds an advantage through its relatively comprehensive legal framework and proactive law enforcement approach, yet continues to face weaknesses in the form of an overly narrow regulatory scope and a regulatory lag relative to technological development. Adaptive regulatory reform and the strengthening of victim protection mechanisms therefore represent urgent imperatives for both countries in effectively combating AI-based Deepfake pornography offenses.

REFERENCES

"2023 State Of Deepfakes: Realities, Threats, And Impact," 2023. https://www.securityhero.io/state-of-deepfakes/#deepfake-porn-survey.

ACT ON SPECIAL CASES CONCERNING THE PUNISHMENT OF SEXUAL CRIMES, Pub. L. No. 20575, Ministry of Government legislation (2025). https://www.law.go.kr/eng/engLsSc.do?menuId=2&query=punishment#liBgcolor7.

Ali, Mahrus, Zico Junius Fernando, Chairul Huda, and Mahmutarom Mahmutarom. "Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims." *Substantive Justice International Journal of Law* 8, no. 1 (May 15, 2025): 1–12. https://doi.org/10.56087/SUBSTANTIVEJUSTICE.V8I1.306.

Andira, Sindi Ayu, and M. Endriyo Susila. "Overcoming Deepfake Porn Crimes In Indonesia." *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 23, no. 1 (June 28, 2024): 2796–2809. https://doi.org/10.31941/PJ.V23I3.4232.

BR, Wahyudi. "Tantangan Penegakan Hukum Terhadap Kejahatan Berbasis Teknologi AI." *Innovative: Journal Of Social Science Research* 5, no. 1 (January 25, 2025): 3436–50. https://doi.org/10.31004/INNOVATIVE.V5I1.17519.

Cheng, Xiangshu. "The Gendered Impact of Deepfake Technology: Analyzing Digital Violence Against Women in South Korea." *Lecture Notes in Education Psychology and Public Media* 75, no. 1 (November 26, 2024): 80–85. https://doi.org/10.54254/2753-7048/75/20241102.

CRIMINAL ACT, Pub. L. No. 19582, Ministry of Government legislation (2023). https://www.law.go.kr/eng/engLsSc.do?menuId=2&query=#liBgcolor10.

Faqih, Muhammad, and Enni Soerjati Priowirjanto. "Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia." *Jurnal Indonesia Sosial Teknologi* 3, no. 11 (November 24, 2022): 1156–68. https://doi.org/10.59141/JIST.V3I11.528.

Geun, Jung Seong, and Jung Jun Seob. *Pengantar Pelajaran Hukum Pidana*. Seoul: Parkyoungsa, 2019.

Haida, Rendi Syaputra Nur, and Eko Nuriyatman. "URGENSI PENGATURAN PERLINDUNGAN HUKUM TERHADAP KORBAN DEEPFAKE MELALUI ARTFICIAL INTELIGENCE (AI) DARI PERSPEKTIF HUKUM PIDANA INDONESIA." *Jurnal Hukum Respublica* 24, no. 01 (December 5, 2024): 1–13. https://doi.org/10.31849/RESPUBLICA.V24I01.23327.

Indonesia, Pemerintah Pusat. "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." Jakarta, 2024. https://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024.

———. "Undang-Undang (UU) Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," 2008. https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008.

Jang, Yujin, and Youngmeen Suh. "Cyber Sex Crimes Targeting Children and Adolescents in South Korea: Incidents and Legal Challenges." *Social Sciences 2024, Vol. 13, Page 596* 13, no. 11 (November 3, 2024): 596. https://doi.org/10.3390/SOCSCI13110596.

Ji, Seung Gyeong. "#MeToo in an AI-Generated Deepfake Sexual Violence Era in South Korea." *Women's Studies International Forum* 112 (September 1, 2025): 103146. https://doi.org/10.1016/J.WSIF.2025.103146.

Joeantito Hartono, Dhimas, and Sugiharto Sugiharto. "THE CRIMINAL RESPONSIBILITY FOR PORNOGRAPHY VIDEO MAKER THROUGH DIGITAL FORENSICS ON SOCIAL MEDIA." *YURIS: Journal of Court and Justice* 1, no. 2 (August 1, 2022): 46–54. https://doi.org/10.56943/JCJ.V1I2.119.

Kim, Hyung-Jin. "South Korea Fights Deepfake Porn with Tougher Punishment and Regulation." AP News, November 6, 2024. https://apnews.com/article/south-korea-deepfake-porn-women-409516f159827770913ddf8d39f84cfd.

Kim, Kyungsuk. "Deepfakes: Challenges to Intellectual Property Rights in South Korea." *GRUR International* 74, no. 6 (July 23, 2025): 532–42. https://doi.org/10.1093/GRURINT/IKAF044.

Komang Suarsika, I, Ni Ketut Wiratny, and Erikson Sihotang. "LEGAL POLICY ON EXHIBITIONISM THROUGH VIDEO CALL-BASED SOCIAL MEDIA REVIEWED FROM THE INFORMATION AND ELECTRONIC TRANSACTIONS (IET) LAW." *IUS POSITUM: Journal of Law Theory and Law Enforcement* 3, no. 2 (August 9, 2024): 48–61. https://doi.org/10.56943/JLTE.V3I2.576.

Kristiyenda, Yoan Shevila, Jasmine Faradila, and Christina Basanova. "Pencegahan

Kejahatan Deepfake: Studi Kasus Terhadap Modus Penipuan Deepfake Prabowo Subianto Dalam Tawaran Bantuan Uang." *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (March 4, 2025): 149–64. https://doi.org/10.59246/ALADALAH.V3I2.1263.

Mandagie, Anselmus S. J. "PROSES HUKUM TINDAK PIDANA PEMBUNUHAN YANG DILAKUKAN OLEH ANAK DIBAWAH UMUR DITINJAU DARI UNDANG-UNDANG NOMOR 11 TAHUN 2012 TENTANG SISTEM PERADILAN PIDANA ANAK." *LEX CRIMEN* 9, no. 2 (May 18, 2020). https://ejournal.unsrat.ac.id/v2/index.php/lexcrimen/article/view/28552.

Nasution, Angelica Vanessa Audrey, Suteki, and Anggita Doramia Lumbanraja. "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse." *International Journal for the Semiotics of Law* 38, no. 7 (October 1, 2025): 2489–2517. https://doi.org/10.1007/S11196-025-10265-0.

Noerman, Chiquita Thefirstly, and Aji Lukman Ibrahim. "Kriminalisasi Deepfake Di Indonesia Sebagai Bentuk Pelindungan Negara." *JURNAL USM LAW REVIEW* 7, no. 2 (June 3, 2024): 603–21. https://doi.org/10.26623/JULR.V7I2.8995.

Pemerintah Pusat Indonesia. "Undang-Undang (UU) Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual." Jakarta, 2022. https://peraturan.bpk.go.id/Details/207944/uu-no-12-tahun-2022.

———. "Undang-Undang (UU) Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Pemerintah Pusat*. Jakarta, November 25, 2016. https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016.

Prayoga, Hendra, and Hadi Tuasikal. "Penyebaran Konten Deepfake Sebagai Tindak Pidana: Analisis Kritis Terhadap Penegakan Hukum Dan Perlindungan Publik Di Indonesia." *Abdurrauf Law and Sharia* 2, no. 1 (May 1, 2025): 22–38. https://doi.org/10.70742/ARLASH.V2I1.194.

Rizki Kurniarullah, Muhammad, Talitha Nabila, Abdurrahman Khalidy, Vivi Juniarti Tan, and Heni Widiyani. "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi." *Jurnal Ilmiah Wahana Pendidikan* 10, no. 10 (June 3, 2024): 534–47. https://doi.org/10.5281/ZENODO.11448814.

Ryu, Bu-gon. "Legal and Institutional Improvement Measures for the Protection of Victims of Deepfake Sex Crimes." 피해자학연구 32, no. 3 (December 31, 2024): 29–56. https://doi.org/10.36220/KJV.2024.32.3.29.

SY, Muhammad Faturrachman. "DEEPFAKE PORNOGRAFI: STUDI KONSTITUSI DAN PENEGAKANNYA DI INDONESIA." *Jurnal Legislatif* 8, no. 2 (January 14, 2025): 113–28. https://doi.org/10.30659/JHKU.V19I4.43173.

Syahirah, Sabrina Nur, and Bayu Prasetyo. "TINJAUAN YURIDIS TERHADAP PENGGUNAAN TEKNOLOGI DEEPFAKE UNTUK PORNOGRAFI MELALUI ARTIFICIAL INTELLIGENCE (AI) DI INDONESIA." *Jurnal Inovasi Hukum Dan Kebijakan* 6, no. 1 (February 13, 2025): 191–212. https://ejurnals.com/ojs/index.php/jihk/article/view/1405.

Truby, Jon. "Governing Artificial Intelligence to Benefit the UN Sustainable Development Goals." *Sustainable Development* 28, no. 4 (July 1, 2020): 946–59. https://doi.org/10.1002/SD.2048;PAGE:STRING:ARTICLE/CHAPTER.